JOURNAL OF ALGEBRA 131, 281–293 (1990)

A Moufang Loop, the Exceptional Jordan Algebra, and a Cubic Form in 27 Variables

ROBERT L. GRIESS, JR.

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109-1003

Communicated by Leonard Scott

Received December 19, 1989

DEDICATED TO WALTER FEIT ON THE OCCASION OF HIS 60TH BIRTHDAY

Let $\mathcal{J}$ be the exceptional 27-dimensional Jordan algebra over $\mathbb{C}$. Its automorphism group is the Lie group $F_4(\mathbb{C})$ and this group is known to have a finite subgroup AL, where A is a self centralizing elementary abelian of order 27, $L \cong SL(3, 3)$, and L normalizes A. As an A-module, $\mathcal{J}$ decomposes into a direct sum of 1-dimensional spaces $\mathcal{J}_x$ which afford the 27 distinct linear characters $x \in A^\wedge := \mathrm{Hom}(A, \mathbb{C}^\times)$. These spaces satisfy $\mathcal{J}_x \mathcal{J}_y = \mathcal{J}_{xy}$. Let $\omega = e^{2\pi i/3}$. There are a basis of $\mathcal{J}$ of the form e_x, for $x \in A^\wedge$, and a function $g: A^\wedge \times A^\wedge \to \mathbb{F}_3$ such that (*) $e_x e_y = (-2)^{-c(x,y)} \omega^{g(x,y)} e_{xy}$, where $c(x, y) = 0$ if x and y are linearly dependent and $c(x, y) = 1$ otherwise. Identifying $A^\wedge$ with $\mathbb{F}_3^3$, we write $x = (x_1, x_2, x_3)$ and $y = (y_1, y_2, y_3)$. A function g which has the above properties is $g(x, y) = -x_1x_2y_3 - x_3y_1y_2 + x_2x_3y_1 + x_1y_2y_3$. The elements $\{e_x \mid x \in A^\wedge\}$ generate the infinite commutative loop $\mathcal{L} := \{(-2)^m \omega^n e_x \mid m \in \mathbb{Z}, n \in \mathbb{Z}_3, x \in A^\wedge\}$ under Jordan multiplication. The loop $\mathcal{L}$ is not Moufang but has as quotient a Moufang loop $\mathcal{M}$ of order 81 and exponent 3. Conversely, the loop $\mathcal{M}$ may be constructed from scratch (using g) and used to define the Jordan algebra $\mathcal{J}$ using the formula (*); this gives a new existence proof for a simple 27-dimensional Jordan algebra over fields of characteristic not 2 or 3 with a primitive cube root of unity (in characteristic 3, we get the group algebra of $A^\wedge$). We discuss some finite groups associated to $\mathcal{M}$ and the Lie groups $F_4(\mathbb{C})$ and $3E_6(\mathbb{C})$ and compare the analogous situation with the loop $\mathbb{O}_{16}$, the Cayley numbers, and Lie groups $G_2(\mathbb{C})$ and $D_4(\mathbb{C})$. We also get a new construction of the cubic form in 27 variables whose group is $3E_6(\mathbb{C})$ and an easy and natural construction of the exotic 3-local subgroup $3^{1+3+3}: SL(3, 3)$.

1. INTRODUCTION

In several papers [GR3], [GR4], [GR5], I have pursued the idea of using loops (nonassociative versions of groups) to describe important and somewhat complicated finite subgroups of sporadic simple groups and Lie groups. In all cases, the loop had 2-power order and was Moufang. I have wanted to find some useful occurrence of other loops, say loops of odd

0021-8693/90 $3.00

order. A natural place to look was at the exceptional 27-dimensional Jordan algebra decomposed with respect to a special group of automorphisms. The rough form of the product $(*)$ was known, but a suitable function g was not; even the degree of such a function was unknown, though obviously it is symmetric since $\mathcal{J}$ is a commutative algebra.

A lecture of Edgar Goodaire at the Canadian Mathematical Society Meeting in Windsor, June, 1989, called my attention to a certain commutative Moufang loop $\mathcal{N}$ of order 81; see [Good]. Marshall Osborn knew this loop very well since he had studied it in his thesis [Os]. Conversations with him made it clear that it had many properties in common with the loop $\mathcal{M}$. Finally, I defined a function g which played the role of a factor set in the construction of $\mathcal{N}$. This g turned out to make the algebra defined by $(*)$ a Jordan algebra. The first proof that this is so is due to a computer program, written by Tom Richardson, for checking the homogeneous form of the standard Jordan identity $ab^2 \cdot b = ab \cdot b^2$; we sketch another proof.

It is a pleasure to acknowledge the contributions of several individuals to our results on $\mathcal{J}$: Arjeh Cohen for showing us his calculations of the representation of $3E_6(\mathbb{C})$ and its subgroup $SL(3, \mathbb{C})^3$ on $\mathcal{J}$; Aloysius (Loek) Helminck for programming efforts to deduce information about g; Edgar Goodaire, for his interesting and timely lecture; Kevin McCrimmon for several clarifying discussions about Jordan algebras; and, especially, Marshall Osborn for sharing his detailed knowledge of the loop $\mathcal{N}$ (described in (2.10), where it is called $\mathcal{M}$).

2. Preliminary Results

(2.1) *Linearized Jordan Identity.* Let x_i, $i = 1, 2, 3, 4$, be nonassociating variables and let $ijkl$ denote a permutation of $(1, 2, 3, 4)$. We let $(ij.k)l$ denote $(x_i x_j . x_k) x_l$ and similarly for other associations. The *linearized Jordan identity* is the identity

$$\begin{aligned}(43.2)1 + (34.2)1 - 43.21 - 34.21 \\ + (13.2)4 + (31.2)4 - 13.24 - 31.24 \\ + (14.2)3 + (41.2)3 - 14.23 - 41.23 = 0.\end{aligned} \tag{2.1.a}$$

For commutative algebras over rings in which 2 is not a zero divisor, this becomes

$$\begin{aligned}(34.2)1 - 34.21 \\ + (13.2)4 - 13.24 \\ + (14.2)3 - 14.23 = 0\end{aligned} \tag{2.1.b}$$

and is equivalent to $(a.a^2)b = a(a^2.b)$; see [Jac, p. 28].

(2.2) DEFINITIONS. A *loop* is a set L with binary operation $L \times L \to L$, written xy or $x.y$, such that

(2.2.a) there is an element $1 \in L$ such that $1x = x = x1$, for all $x \in L$, and

(2.2.b) given $x \in L$, there are $y, z \in L$ such that $xy = 1 = zx$.

The *nucleus* of L is $\mathrm{Nuc}(L) := \{x \in L \mid ax.b = a.xb,\ xa.b = x.ab,$ and $ab.x = a.bx$, for all $a, b \in L\}$ and the *center* is $Z(L) := \{z \in \mathrm{Nuc}(L) \mid za = az$, for all $a \in L\}$. See [Br]. The *commutator* (a, b) of elements a, b is defined by $ab = ba.(a, b)$. The *associator* (a, b, c) of elements a, b, c is defined by $ab.c = (a.bc)(a, b, c)$.

(2.3) *Remark.* The rule $(xy)^{-1} = y^{-1}x^{-1}$ holds if 2-generator subloops are associative.

(2.4) DEFINITION. The loop L is *Moufang* if one (hence all) of the following identities holds:

$$xy.zx = (x.yz)x; \tag{2.4.a}$$

$$(xy.z)\ y = x(y.zy); \tag{2.4.b}$$

$$x(y.xz) = (xy.x)z. \tag{2.4.c}$$

In a Moufang loop, 2-generator subloops are groups, so (2.3) is relevant. See [Br] for generalities about loops and a summary of basic Moufang theory.

(2.5) DEFINITION. Given loops L and M, an *extension* is a loop E which participates in a short exact sequence $1 \to L \to E \to^{\pi} M \to 1$.

Given $f: M \times M \to L$, we may construct an E as the set $L \times M$ with product $(a, x) * (b, y) = (ab.f(x, y), xy)$. Then E is a loop. Given an extension, we choose a *transversal*, i.e., an element $u(x) \in E$ for each $x \in M$ such that $u(x)\pi = x$, for all x; we then use (2.2.b) here to get a factor set $f(x, y)$, defined by $u(x)u(y) = f(x, y)u(xy)$.

(2.6) *Notation.* $V = \mathbb{F}_3^3$; we let x_i be the ith coordinate of $x \in V$. Let

$$\Delta = \Delta(x, y, z) = \det \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix}, \qquad \text{for} \quad x, y, z \in V.$$

(2.7) *Notation.* Let $\{i, j, k\} = \{1, 2, 3\}$ and let $L_{ij} = L_{ji}$, $R_{ij} = R_{ji}$ be the functions which send (x, y) to $x_i x_j y_k$, $x_k y_i y_j$, respectively.

We use the usual definition of coboundary from cohomology of groups. This notion may be applied to scalar-valued functions whose arguments lie in V. Since we act on the right, if $h: G \times G \to A$ where A is a module, $(\delta h)(x, y, z) = h(x, y) + h(xy, z) - h(y, z)^{x^{-1}} + h(x, yz)$. Here, $G = V$ and $A = \mathbb{F}_3$ is a trivial module.

(2.8) LEMMA (Some Coboundary Calculations). *We have*

(i) $(\delta L_{ij})(x, y, z) = x_i y_j z_k + x_j y_i z_k$.

(ii) $(\delta R_{ij})(x, y, z) = -x_k y_i z_j - x_k y_j z_i$.

Proof. Let $g = L_{ij}$. Then $g(x, y) + g(x + y, z) = x_i x_j y_k + (x_i + y_i)(x_j + y_j) z_k = x_i x_j y_k + x_i x_j z_k + x_i y_j z_k + y_i x_j z_k + y_i y_j z_k$ and $g(y, z) + g(x, y + z) = y_i y_j z_k + x_i x_j y_k + x_i x_j z_k$ whence (i). Let $g = R_{ij}$. Then $g(x, y) + g(x + y, z) = x_k y_i y_j + x_k z_i z_j + y_k z_i z_j$ and $g(y, z) + g(x, y + z) = y_k z_i z_j + x_k (y_i + z_i)(y_j + z_j) = y_k z_i z_j + x_k y_i y_j + x_k y_i z_j + x_k y_i z_j + x_k z_i z_j$, whence (ii). ∎

(2.9) PROPOSITION (Existence of a Good Factor Set). *Take* $g = -L_{12} + R_{23} + L_{23} - R_{12}$. *Then* $\delta g = \Delta$.

Proof. Let the symbol ijk stand for the monomial $x_i y_j z_k$. Using (2.3), we compute $\delta g = -123 - 213 - 123 - 132 + 231 + 321 + 312 + 321 = 123 + 231 + 312 - 213 - 132 - 321 = \Delta$. ∎

(2.10) DEFINITION (The Loop $\mathscr{M}$). We let $\mathscr{M}$ be the loop which is a central extension $1 \to \mathbb{F}_3 \to \mathscr{M} \to \mathbb{F}_3^3 \to 1$ with structure given by the factor set g from (2.9).

(2.11) LEMMA. *The loop* $\mathscr{M}$ *is commutative, Moufang, and non-associative, whence all associators generate* $Z(\mathscr{M}) \cong \mathbb{Z}_3$. *In fact, the associator of* $(*, x)$, $(*, y)$, *and* $(*, z)$ *in* $\mathscr{M}$ *is* $(\Delta, 0)$.

Proof. Commutativity follows since the symbols R and L occur symmetrically in the definition of g. We compute that the associator of these three elements is $(g(x, y) + g(x + y, z) - g(y, z) - g(x, y + z), 0)$, which by (2.9) equals $(\Delta(x, y, z), 0)$.

To verify the Moufang identity, we get the requirement $(g(x, y) + g(z, x) + g(x + y, z + x), 0) = (g(y, z) + g(x, y + z) + g(x + y + z, x), 0)$ from (2.4.a). This is proved by adding the two expressions below for associators of (i), $(0, x)$, $(0, y)$, and $(0, z)$; (ii) $(0, u)$, $(0, z)$ and $(0, x)$, where u stands for $x + y$:

(i) $g(x, y) + g(x + y, z) - \Delta(x, y, z) = g(y, x) + g(x, y + z)$

(ii) $g(z, x) + g(u, z + x) = g(u + z, x) + g(u, z) - \Delta(u, z, x)$. ∎

(2.12) *Extraspecial Groups and Their Faithful Modules* (Adapted from Sect. 3 of [Gr6]). Let Q be an extraspecial group of order p^{1+2n} and of plus type. Given a nontrivial linear character λ on $Z(Q)=\langle z\rangle$, there is a unique irreducible module T for Q such that z acts as $\lambda(z)$. Let $Q=EF$ be factorized into elementary abelian groups E and F of orders p^{1+n} and p^n, respectively. Then, there is a basis $\{e(x)\mid x\in F\}$ of T such that $e(x)^y=e(xy)$ for $y\in F$ and $e(x)^y=\varphi(y)e(x)$ for $y\in E$, where φ is defined by $\varphi(y):=\lambda([x,y])$. Let $\{f(x)\mid x\in F\}$ be the dual basis of the dual module. The space $T\otimes T^*$ has the structure of the associative ring of degree n matrices by the rule $e(u)\otimes f(v)\cdot e(w)\otimes f(x)=\delta_{v,w}e(u)\otimes f(x)$. For a linear character φ of Q, let φ denote an element of Q such that $\lambda([q,\varphi])=\varphi(q)$, for all $q\in Q$; this determines only the coset of $Z(Q)$ containing φ. Also, let x_φ be that element of F such that $\varphi^{-1}x_\varphi\in C(E)=E$.

Now let p be an odd prime. Let $\varepsilon(a,b):=\lambda([a,b])^k$, where $2k\equiv 1 \pmod p$; ε is alternating, bilinear, and nonsingular. The elements $A_\varphi:=\sum_{x\in F}\varepsilon(\varphi,x)e(x)\otimes f(xx_\varphi)$ are eigenvectors for the linear characters of Q on $T\otimes T^*$ and they satisfy the rule $A_\varphi A_\psi=\varepsilon(\varphi,\psi)A_{\varphi\psi}$. Since ε is a bimultiplicative map $Q/Q'\times Q/Q'\to\langle\zeta\rangle$, where ζ is a primitive pth root of unity, essentially detecting commutation, we have that $\varepsilon(a,b)+\varepsilon(b,a)=2$ or $\mu+\mu^{-1}$ as a and b commute or not, where μ is some primitive pth root of unity.

Now, let $p=3$. In the above, $\mu+\mu^{-1}=-1$. Therefore, if we make $T\otimes T^*$ into a Jordan algebra by the symmetrized product $A\circ B:=(AB+BA)/2$, we get that $A_\varphi\circ A_\psi=A_{\varphi\psi}$ or $-\frac{1}{2}A_{\varphi\psi}$, according to whether φ and ψ commute or not. When $n=1$, this last dichotomy amounts to whether φ and ψ are linearly dependent or not (as linear characters, or as elements of Q/Q').

3. Groups of Exponent 3 and Loops

(3.1) Proposition. *Let $B(3,d)$ be the quotient of the free group on $d\geqslant 1$ generators by the subgroup generated by cubes.* Then $|B(3,d)|=3^{d+\binom{d}{2}+\binom{d}{3}}$, *where $\binom{n}{r}=0$ if $r>n$. The ascending and descending central series coincide and the factors of the descending series are elementary abelian of ranks d, $\binom{d}{2}$ and $\binom{d}{3}$, respectively. Thus, G has nilpotence class 1 if $d=1$, 2 if $d=2$, and 3 if $d\geqslant 3$.*

Proof. See [Hall]. ∎

(3.2) Definition. Let $G=B(3,d)$ and let G_i, $i\geqslant 1$, be the lower central series. Choose generators x_i, $i=1,\ldots,d$. Define $x_{ij}:[x,x]$ and $x_{ijk}:=[x_i,x_{jk}]$. Since $\mathrm{cl}(G)\leqslant 3$, G_2 is abelian. Also, 2-generator subgroups

are of class 2 and every pair of conjugate elements commutes. The *coordinates* of $g \in G$ are the elements in the triple (a, b, c), where $g = abc$, $c \in C_d$, a transversal to G_2 in G, $b \in \langle x_{ij} \mid i, j = 1, ..., d \rangle \cong 3^{\binom{d}{2}}$, and $a \in \langle x_{ijk} \mid i, j, k = 1, ..., d \rangle \cong 3^{\binom{d}{3}}$; note that those g with $a = c = 1$ form the fixed points of the automorphism which inverts each x_j. The coordinates are uniquely determined. Let $A = A_d$ be the set of all g with $b = c = 1$ and define $B = B_d$, C_d analogously; then $C = C_d$. For $c, c' \in C$, let $\overline{cc'}$ be that element of C which is congurent to cc' modulo G_2. Require $1 \in C_d = C_d^{-1}$.

We may identify G_2/G_3 with the exterior square of the vector space G_1/G_2 and thereby write the group law multiplicatively as follows: let $g = (a, b, c)$ and $g' = (a', b', c')$; then $gg' = (aa'[c, b']h(c, c'), bb' \cdot k(c, c'), \overline{cc'})$, for some function $h: C_d \times C_d \to A_d$ and that bilinear $k: C_d \times C_d \to B_d$ which satisfies $k(c, c')^{-1} = c \wedge c'$. Let Δ be the alternating trilinear function from G/G_2 to G_3 such that $\Delta(x_i, x_j, x_k) = x_{ijk}$.

(3.3) DEFINITION. Let $G = B(3, d)$; see (3.1). Assume we have chosen a set of generators and so have a coordinate system in the sense of (3.2). Let $V = \mathbb{F}_3^d$ and $U = \mathbb{F}_3^{\binom{d}{3}}$; we continue to write the group law multiplicatively. The *associated Moufang loop* is the loop $\mathcal{N}_d$ whose underlying set is $U \times V$ with product $(a, c) * (a', c') = (aa'h(c, c'), cc')$, where h is as in (3.3). Define $\mathcal{M} := \mathcal{N}_3$; as a set, this is $\mathbb{F}_3 \times \mathbb{F}_3^3$.

(3.4) LEMMA (Properties of $\mathcal{N}_d$). (i) *h is symmetric, whence $\mathcal{N}_d$ is commutative*; (ii) *$\delta h = \Delta$ (see (2.6))*; (iii) *Δ gives associators in $\mathcal{M}$ of $(*, u)$, $(*, v)$ and $(*, w)$*; (iv) *$\mathcal{N}_d$ is commutative and Moufang.*

Proof. (i) If $c \in C_d$, $x, y \in \langle c \rangle$, then $\bar{x}\bar{y} = \overline{xy}$ and $h(x, y) = 1$. The inversion map on C_d extends to an automorphism of G, whence $h(x^{-1}, y^{-1}) = h(x, y)^{-1}$ for $x, y \in C_d$. Easily, we check $(a, b, c)^{-1} = (a^{-1}[c, b], b^{-1}, c^{-1})$. Computing $(1, 1, y^{-1})(1, 1, x^{-1}) = ((1, 1, x)(1, 1, y))^{-1}$ in two different ways, we get $h(x, y) = h(y, x)$.

(ii) follows from a straightforward evaluation of $(a, b, c)(a', b', c')$ (a'', b'', c'') with the two different associations.

(iii) is straightforward.

(iv) The Moufang identity follows from the fact that Δ is trilinear. ∎

(3.5) *Notation.* We define a 27-dimensional space by taking the algebra $\mathbb{C}[\mathcal{M}]$ with basis $\mathcal{M}$ and set $\mathcal{J} := \mathbb{C}[\mathcal{M}]/\mathbb{C}[\mathcal{M}](\omega - z)$, where $\omega := e^{2\pi i/3}$ and z denotes the generator $(1, 0)$ of $Z(\mathcal{M})$. Let e_x denote the image in $\mathcal{J}$ of $x \in \mathcal{M}$. Then $e_{zx} = \omega e_x$, for all x, so that we have a triple basis. Let $\lambda: \mathcal{M} \to \langle \omega \rangle$ be defined by $\lambda(z^i) = \omega^i$ and $\lambda(x) = 0$ for x noncentral.

(3.6) AFFINE TRANSFORMATIONS ON $\mathscr{M}$. *Let ρ_a be the map $x \mapsto xa$ on $\mathscr{M}$ and let $\delta_{a,b}$ be the map $x \mapsto z^{\Delta(x,a,b)}$. Then* (i) $\rho_a\rho_b = \rho_{ab}\,\delta_{a,b}$; (ii) $\rho_c\,\delta_{a,b} = \delta_{a,b}\,\rho_c\rho_z^{\Delta(c,a,b)}$.

Proof. (i) For $x \in \mathscr{M}$, $x\rho_a\rho_b = xa.b = x.ab.z^{\Delta(x,a,b)} = x\rho_{ab}\delta_{a,b}$. (ii) For $x \in \mathscr{M}$, $x\rho_c\delta_{a,b} = (xc)\delta_{a,b} = xc.z^{\Delta(xc,a,b)} = xz^{\Delta(x,a,b)}cz^{\Delta(c,a,b)} = x\delta_{a,b}\rho_c\rho_z^{\Delta(c,a,b)}$. ∎

(3.7) *Remark* (Automorphism Group of $\mathscr{M}$). Since $\mathrm{Aut}(\mathbb{F}_3^3)$ preserves the function δh, which gives associators, $\mathrm{Aut}(\mathscr{M})$ is part of a short exact sequence $1 \to \mathrm{Diag}(\mathscr{M}) \to \mathrm{Aut}(\mathscr{M}) \to GL(3,3) \to 1$, where $\mathrm{Diag}(\mathscr{M}) \cong \mathbb{F}_3^3$ is the set of automorphisms trivial on $\mathscr{M}/Z(\mathscr{M})$ (note that the action of $\mathrm{Aut}(\mathscr{M})$ on the center of $\mathscr{M}$ is by the determinant). We get splitting of this sequence by quoting either [Sah] or [Gr1]; we get nowhere by taking the centralizer of an involutory automorphism which inverts $\mathscr{M}/Z(\mathscr{M})$ since it inverts $\mathscr{M}$ and so is in $Z(\mathrm{Aut}(\mathscr{M}))$.

(3.8) *Cohomologousness of g and h.* Since $\delta g = \Delta = \delta h$, if we use $g - h$ in (3.3), we get an abelian group. Since g and h vanish if their arguments are dependent, the group is elementary abelian, whence $g - h$ is cohomologous to 0.

4. JORDAN ALGEBRAS: EXAMPLES AND CLASSIFICATION

The next two results are mentioned for background.

(4.1) THE SIMPLE JORDAN ALGEBRAS. *Let K be an algebraically closed field of characteristic not 2 and let $\mathscr{J}$ be a finite dimensional simple Jordan algebra over K. Then $\mathscr{J}$ is isomorphic to one of the following.*

(4.1.a) $\mathrm{Mat}_n(K)^+$, *dimension n^2.*

(4.1.b) $\mathrm{Sym}_n(K)^+$, *the symmetric matrices of degree n, dimension $n(n-1)/2$;*

(4.1.c) $\{x \in \mathrm{Mat}_{2m}(K) \mid x^J = x\}$, *where $x^J = q^{-1}\,{}^t\!xq$, where $q = \left(\begin{smallmatrix} 0 & I_m \\ -I_m & 0 \end{smallmatrix}\right)$, dimension $2m^2$;*

(4.1.d) *an algebra with basis s_i, $i = 0, \ldots, n$, and defining relations $s_0 s_i = s_i$, $i = 1, \ldots, n$, $s_i s_j = \delta_{ij} s_0$;*

(4.1.e) *the exceptional Jordan algebra, given by, say, 3×3 Hermitean matrices over the Cayley numbers.*

(4.2) MAXIMAL SUBALGEBRAS OF $\mathscr{J}$. *Let $\mathscr{B}$ be a subalgebra of $\mathscr{J}$. Then $\mathscr{B}$ is maximal iff $\mathscr{B}$ is isomorphic to one of the following:*

(4.2.1) $\mathbb{C}e \oplus \mathscr{J}_0(e)$, *for a primitive idempotent, e;*

(4.2.2) $\mathscr{H}(\mathscr{S}_3)$, *where* $\mathscr{S}$ *is a certain maximal subalgebra of an octonian algebra*;

(4.2.3) $\mathscr{J}(\mathbb{C}z)$, *the idealizer of* $z \in \mathscr{J}$, *where*, $z \neq 0 = z^2$.

(*See* [Rac2] *for notation*). *The respective dimensions are* 11, 21, *and* 18.

Proof. [Rac2].

(4.3) *A One-Parameter Family of* 27*-Dimensional Algebras.* Let A be an elementary abelian group of order 27 and $A^\wedge$ its group of characters. For $\alpha \in \mathbb{C}^\times$, we let $\mathscr{E}(\alpha, c, g)$ be the algebra with basis e_μ, $\mu \in A^\wedge$ and with product $e_\mu * e_\nu = \alpha^{c(\mu,\nu)}\omega^{g(\mu,\nu)}e_{\mu\nu}$, where $c(\mu, \nu) = 0$ or 1 as $\mu \wedge \nu$ is 0 or not and where g is given in (2.9). Then:

(4.3.a) $\mathscr{E}(-\frac{1}{2}, c, g)$ is a Jordan algebra;

(4.3.b) $\mathscr{E}(1, c, g)$ is not a Jordan algebra;

(4.3.c) $\operatorname{span}\{e_\mu \mid \mu \in U\}$ (considered as a subalgebra of $\mathscr{E}(1, c, g)$) is a Jordan algebra, if U is any rank 2 subspace of $A^\wedge$; it is the simple algebra (4.1.d) of dimension 9. (By (4.2), it is not a maximal subalgebra.)

These statements were proved by verifying the linearized Jordan identity (2.1.b). I thank Tom Richardson for writing a program to perform the necessary checking of all possible substitutions of e_as in (2.1.b). An alternative proof of a more general result is sketched later, in (4.5).

(4.4) PROPOSITION. *Let* c *and* g *be as in* (4.3) *with* $\alpha = -\frac{1}{2}$ *and let* g_U *be the restriction of* g *to* $\operatorname{span}\{e_\mu \mid \mu \in U\}$, *where* U *is any rank* 2 *subspace of* $A^\wedge$. *Then* g_U *is cohomologous to* 0.

Proof. Let $\mathscr{K} := \operatorname{span}\{e_\lambda \mid \lambda \in U\}$. We observe that $\mathscr{K}$ has the triple basis $\{e_x \mid x \in \mathscr{P}\}$, where $\mathscr{P}$ is the subloop of $\mathscr{M}$ of index 3 corresponding to U in $A^\wedge$. The relations are $e_{zx} = \omega e_x$. In the associated Burnside group G (see (3.2)), the function h may be altered by choosing a different transversal to G_2 in G. Since 2-generator subgroups of G are extraspecial of order 27, the function h when restricted to U may be made identically 0 by a good choice of transversal, and this proves g is cohomologous to 0. ∎

(4.5) PROPOSITION. *In the notation of* (4.3), $\mathscr{E}(\alpha, c, g)$ *is a Jordan algebra iff* $\alpha = -\frac{1}{2}$.

Proof (Sketch Only). Note that for any such algebra, $\operatorname{Aut}(\mathscr{M})$ operates as automorphisms. We study (2.1.b) here, and use variables a, b, c, d which run over the triple basis $\{e_x \mid x \in \mathscr{M}\}$.

Case 1. The images of a, b, c, d in $\mathscr{M}/Z(\mathscr{M}) \cong \mathbb{F}_3^3$ span a space of dimension at most 2. By (4.4), we may assume all relevant values of g here

are 0. We assume that the images of two of these in $\mathscr{M}/Z(\mathscr{M})$ are (100) and (010). Say $a \mapsto (100)$, $b = c = d \mapsto (010)$. Substitution gives the condition $(\alpha - 1)^2 (2\alpha + 1) = 0$, which means that the only good values of α can be 1 or $-\frac{1}{2}$. Further work here will not eliminate $\alpha = 1$.

Case 2. The first variable is central. In this case, the monomials in (2.1.b) cancel formally.

Case 3. A set of three of the variables (including the first) are independent modulo $Z(\mathscr{M})$. We may assume that they correspond to (100), (010), and (001). The fourth corresponds to (pqr) and so there are just 27 substitutions to check. ∎

(4.6) *Notation.* $\mathscr{J} := \mathscr{E}(-\frac{1}{2}, c, g)$.

5. $\mathscr{M}$, $\mathscr{J}$, $F_4(\mathbb{C})$, AND $3E_6(\mathbb{C})$.

In this section, we study invariant cubic forms on $\mathscr{J}$ and on certain 9-dimensional subalgebras.

(5.1) *Notation.* For $a, b \in \mathscr{M}$, $\Delta(a, b) = 1$ or 0 as a and b are congruent or not modulo $Z(\mathscr{M})$. Define $\Delta_{a,b,c,\ldots} := \Delta_{a,b}\,\Delta_{a,c}\,\Delta_{a,d}\cdots$.

(5.2) *Notation.* $\theta_1(e_a, e_b, e_c) := \Delta_{abc,1}(\Delta_{1,a} + \Delta_{1,b} + \Delta_{1,c})\,\lambda(abc)$, where λ is defined in (3.6);

$$\theta_2(e_a, e_b, e_c) := \Delta_{abc,1}\,\lambda(abc);$$
$$\theta_3(e_a, e_b, e_c) := \Delta_{a,b,c}\,\lambda(abc);$$
$$\theta_4(e_a, e_b, e_c) := \Delta_{1,a,b,c}\,\lambda(abc).$$

(5.3) DEFINITION. Let G be the subgroup of $GL(\mathscr{J})$ generated by $B := \mathrm{Aut}(\mathscr{M})$ and R the group generated by all right multiplications by $\mathscr{M}$ on the indices; that is, $R := \langle \rho_x \mid x \in \mathscr{M} \rangle$, where $\rho_x : e_y \mapsto e_{xy}$. For a subloop $\mathscr{U}$ of $\mathscr{M}$, we let $R_{\mathscr{U}} := \langle \rho_x \mid x \in \mathscr{U} \rangle$ and $B_{\mathscr{U}} := \{ g \in B \mid g \text{ stabilizes } \mathscr{U} \}$.

(5.4) PROPOSITION. (i) *The space of B-invariant cubic forms is spanned by* $\theta_1, \theta_2, \theta_3, \theta_4$.

(ii) *The cubic forms* θ_2 *and* θ_4 *are preserved by G and span the space of all G-invariant cubic forms.*

Proof. (i) is trivial.

(ii) The actions of G as AGL(3, 3) on the 27 one-spaces and of $\mathrm{Diag}(\mathscr{M})$ on the individual one-spaces make it clear that the space of invariant cubic forms is at most 2-dimensional.

Take $a, b, c, x \in \mathscr{M}$. Since $\Delta_{abc,1} = \Delta_{ax\cdot bx\cdot cx,1}$, it remains to be shown that $abc = ax\cdot bx\cdot cx$ when all these are in $Z := Z(\mathscr{M})$. This follows from commutativity and use of the Moufang identity. Let $w := abc \in Z$. We compute $(ax\cdot bx)\,cx = (xa\cdot bx)\,cx = yx\cdot cx$, by (2.4a), with $y = x\cdot ab$. Now, $yx\cdot cx = xy\cdot cx = (x\cdot yc)x$, by (2.4.a). Since 2-generator subloops are associative, $yc = (x\cdot ab)c = x(ab\cdot c) = xw$ and so $(ax\cdot bx)cx = x^3w = w$, as required. ∎

We want to give a cubic form on the vector space $\mathscr{J}$ which is invariant under a copy of $3E_6(\mathbb{C})$.

(5.5) LEMMA. *Let $\mathscr{U}$ be an index 3 subloop of $\mathscr{M}$, $\mathscr{U} = \mathbb{F}_3 \times U \leqslant \mathscr{M}$ and let $\mathscr{K}$ be the subalgebra span $\{e_x \mid x \in \mathscr{U}\}$. Then:*

(i) *$g|_{U\times U}$ is cohomologous to 0 and $\mathscr{K}$ is isomorphic to the simple Jordan algebra $\mathrm{Mat}_3(\mathbb{C})^+$; there is an isomorphism in which our triple basis corresponds to $\{\omega^p A^q B^r \mid p, q, r = 0, 1, 2\}$, where*

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \bar{\omega} \end{pmatrix}.$$

Also, $B_{\mathscr{U}} := \mathrm{Stab}_B(\mathscr{U})$ acts on $\mathscr{K}$ as $3^2{:}\,GL(2, 3)$ with kernel 3^3.

(ii) *$\mathscr{K}$ has a 3-dimensional space of $\mathrm{Aut}(\mathscr{K})$-invariant cubic forms with basis g_1, g_2, g_4, where g_i is the restriction to $\mathscr{K}$ of θ_i; they correspond to scalar multiples of cubic forms f_i on $\mathrm{Mat}_3(\mathbb{C})^+$, where $f_1(A, B, C) = \mathrm{tr}(A)\,\mathrm{tr}(B\circ C) + \mathrm{tr}(B)\,\mathrm{tr}(C\circ A) + \mathrm{tr}(C)\,\mathrm{tr}(A\circ B)$ (here $A\circ B$ is the Jordan product $\frac{1}{2}(AB + BA)$), $f_2(A, B, C) = \mathrm{tr}((A\circ B)\circ C)$, and $f_4(A, B, C) = \mathrm{tr}(A)\,\mathrm{tr}(B)\,\mathrm{tr}(C)$;*

(iii) *The space of cubic forms in $\mathrm{span}\{g_1, g_2, g_4\}$ invariant under $R_{\mathscr{U}}$ is $\mathrm{span}\{g_2\}$.*

Proof. (i) Follows from (2.12), (3.8), and (4.4).

(ii) We may imitate the argument of (5.4) to get that the space of $B_{\mathscr{U}}$-invariant forms is 4-dimensional. From (5.2) and (5.4), the space of $\mathrm{Aut}(\mathscr{K})$-invariant cubic forms contains $\mathrm{span}\{g_1, g_2, g_4\}$. Since $B_{\mathscr{U}} \leqslant \mathrm{Aut}(\mathscr{K})$, we show that the space is no larger by showing that θ_3 restricts to 0. Let $D = \mathrm{diag}(-1, 1, 1)$ and compute that $C := D^{-1}ABD = \frac{1}{3}[2\omega A - BA + 2\bar{\omega}B^2A]$, $\theta_1(AB, AB, AB) = 1$ and $\theta_1(C, C, C) = \frac{1}{9}[4\bar{\omega} + 1 + 4\omega] = -\frac{1}{3}$, whence invariance fails.

(iii) It suffices to show that if a linear combination $h = \alpha g_1 + \beta g_4$ is invariant, it is 0. Let a and b be elements of $\mathscr{U}$ which are independent modulo the center. Then, using ρ_a, we get $h(e_1, e_b, e_{b^{-1}}) = h(e_a, e_{ba}, e_{b^{-1}a})$ and $\alpha = 0$; also, $h(e_1, e_1, e_1) = h(e_a, e_a, e_a)$, whence $\beta = 0$. ∎

(5.6) COROLLARY. (i) *The space of cubic forms on $\mathcal{J}$ invariant under* $\mathrm{Aut}(\mathcal{J})$ *is 3-dimensional.*

(ii) *The space of cubic forms on $\mathcal{J}$ which is invariant under* $\langle G, \mathrm{Aut}(\mathcal{J})\rangle$ *is spanned by* θ_2.

Proof. Let $(\cdot,\cdot)$ be the bilinear form based on $u, v \mapsto \mathrm{tr}(\mathrm{ad}(u)\,\mathrm{ad}(v))$. The space of $\mathrm{Aut}(\mathcal{J})$-invariant cubic forms is at least 3-dimensional since it contains $(u, v, w) \mapsto (1, u)(1, v)(1, w)$, $(1, u)\,\mathrm{tr}(\mathrm{ad}(v)\,\mathrm{ad}(w)) + (1, v)\,\mathrm{tr}(\mathrm{ad}(w)\,\mathrm{ad}(u)) + (1, w)\,\mathrm{tr}(\mathrm{ad}(u)\,\mathrm{ad}(v))$, and $\mathrm{tr}((\mathrm{ad}(u)\,\mathrm{ad}(v)) \circ \mathrm{ad}(w))$. To prove (i), use (5.4.i) and (5.5.ii). To prove (ii), use (5.5.iii), the facts that a G-invariant form is determined by its values on triples (e_a, e_b, e_c) with $abc = 1$ and that $\mathcal{U}$ contains an R-orbit of $\{a, b, c\}$ for any such triple. ∎

(5.7) PROPOSITION. *Up to isomorphism, there is a unique group H which satisfies these conditions*:

(5.7.a) $R := O_3(H)$ *has class* 3, *exponent* 3, *and order* 3^7.

(5.7.b) $H/R \cong SL(3, 3)$ *and R/R' is a faithful* 3*-dimensional module for* H/R.

(5.7.c) *There is a transversal $\mathcal{T}$ to R' in R such that* $S := N_H(\mathcal{T} \bmod Z(R))$ *satisfies* $SR = H$ *and* $S \cap R = R'$.

Proof. Let $K = H/Z(R)$ and note that $Z(R) = Z(H)$. Since $SL(3, 3)$ has trivial Schur multiplier [St] and since the first two terms of the descending central series of R are non-self dual and absolutely irreducible H/R-modules, it follows that K has Schur multiplier of order at most 3. Since H is perfect, a result of Schur implies that the uniquely determined covering group of H [Hup], whence it suffices to prove uniqueness of K. The isomorphism type of R, hence $R/Z(R)$, is determined since $R \cong B(3, 3)$. From (5.7.c), we see that the action of S on K is thus uniquely determined. Since $H^2(SL(3, 3), V) = 0$ if V is a 3-dimensional module for $\mathbb{F}_3[SL(3, 3)]$ [Gr1, Sah], S splits over $R/Z(R)$ and so the extension type of K is determined. ∎

(5.8) COROLLARY. *G embeds in $3E_6(\mathbb{C})$, and this embedding is unique up to conjugacy in* $3E_6(\mathbb{C})$.

Proof. By (5.7), it suffices to find a subgroup of $3E_6(\mathbb{C})$ which satisfies (5.7.a, b, and c). See [Gr4] Table 2. The existence of $\mathcal{T}$ as in (5.7.c) follows from the fact that an outer automorphism γ of $3E_6(\mathbb{C})$ may be arranged to normalize a subgroup H of the form 3^{1+3+3}: $SL(3, 3)$, centralize $H/O_3(H)$, and so invert the Frattini factor of $O_3(H)$ (see [Gr4] (2.18)). We take $\mathcal{T}$ to be the set of elements inverted by γ. ∎

(5.9) PROPOSITION. *The group* $3E_6(\mathbb{C})$ *has two nontrivial modules of dimension* 27 (*one is the dual of the other and both are irreducible*). *On each, there is a unique* (*up to scalar*) *invariant cubic form. A nontrivial* 27*-dimensional module for the group* $F_4(\mathbb{C})$ *has an essentially unique invariant Jordan algebra structure*; *its automorphism group is* $F_4(\mathbb{C})$.

Proof. Well-known. ∎

(5.10) PROPOSITION. *The subgroup of* $GL(\mathcal{J})$ *which leaves the above cubic form invariant is isomorphic to* $3E_6(\mathbb{C})$.

Proof. First argument. Use (5.8) to get $G \leqslant G^* \cong 3E_6(\mathbb{C})$. Let $F_4(\mathbb{C}) \cong K \leqslant G^*$ such that $K \cap G = B$. Then use (5.6.ii) and (5.9).

Second argument. By (5.6.ii), $\langle G, \mathrm{Aut}(\mathcal{J}) \rangle$ preserves a nonzero cubic form θ. Since $L := \mathrm{Aut}(\theta)$ is an algebraic group with $L^0 \neq 1$ and is irreducible (since G is), we conclude that L^0 is quasisimple with $L^0 \cap \{\text{scalars}\} = \langle \omega \cdot \mathrm{Id}_{\mathcal{J}} \rangle \cong \mathbb{Z}_3$. We use the classification of quasisimple algebraic groups to conclude that $L \cong 3E_6(\mathbb{C})$ and that L is generated by G and $\mathrm{Aut}(\mathcal{J})$. (It helps to locate G on Table 2 of [Gr4] and note that $Z(O_3(G))$ is not in a torus [else the torus would fix each of the 1-spaces spanned by the e_a; for some a, $\mathbb{C}e_a$ is a nontrivial module for the torus, but this is impossible since $\theta(e_a, e_a, e_a) \neq 0$]). ∎

6. $\mathbb{O}_{16}$, CAYLEY NUMBERS, $G_2(\mathbb{C})$, AND $D_4(\mathbb{C})$.

The techniques of this paper have analogues for the prime 2, which were explored in [Gr5].

In [Cox], it is shown that there is a loop of 16 elements, which we call $\mathbb{O}_{16}$, which forms a double basis of $\mathscr{C}$, the 8 dimensional Cayley algebra. The seven maximal subloops of $\mathbb{O}_{16}$ are quaternion groups of order 8 and the subalgebras of $\mathscr{C}$ they span are quaternion algebras. The group $2^3 \cdot GL(3, 2) \cong \mathrm{Aut}(\mathcal{O})$ is embedded in $\mathrm{Aut}(\mathscr{C}) \cong G_2(\mathbb{C})$ and the group generated by right multiplications with $\mathcal{O}$ and $\mathrm{Aut}(\mathcal{O})$ is of the form $2^{1+3+3} \cdot GL(3, 2)$. This group is involved in a larger finite group of the form $2^{2+3+3} \cdot [GL(3, 2) \times \sum_3] \leqslant \mathrm{Spin}(8, \mathbb{C}) : \sum_3$; see [Gr3, Gr5] for details.

The procedure of "removing the middle" of the group $B(3, 3)$ in (3.2) to get the function h and ultimately the Jordan algebra has an analogue for the prime 2.

ACKNOWLEDGMENTS

This research was supported in part by several NSF grants and by the University of Michigan, the Centre Nationale de Recherche Scientifique de France, and the École Normale Supérieure.

REFERENCES

[Br] R. H. BRUCK, "A Survey of Binary Systems," Springer-Verlag, Berlin, 1958.
[Cox] H. S. M. COXETER, Integral Cayley numbers, *Duke Math. J.* **13** (1946), 561–578.
[Good] E. GOODAIRE, Circle loops of radical alternative rings, *Algebras Groups Geom.* **4** (1987), 461–474.
[Gr1] R. L. GRIESS, JR., Splitting of extensions of $SL(3, 3)$ by the vector space $\mathbb{F}_3^3$, *Pacific J. Math.* **63** (1976), 405–409.
[Gr2] R. L. GRIESS, JR., Code loops, *J. Algebra* **100** (1986), 224–234.
[Gr3] R. L. GRIESS, JR., Sporadic groups, code loops and nonvanishing cohomology, *J. Pure Appl. Algebra* **44** (1987), 191–214.
[Gr4] R. L. GRIESS, JR., Elementary abelian p-subgroups of Lie groups, preprint.
[Gr5] R. L. GRIESS, JR., Code loops and a large finite group containing triality for D_4, *in* "Atti del Convegno Internazionale di Teoria dei gruppi e Geometria Combinatoria, Firenze, 23-22 Ottobre, 1986," *Rend. Circ. Mat. Palermo (2) Suppl.*, 79–98.
[Gr6] R. L. GRIESS, JR., The friendly giant, *Invent. Math.* **69** (1982), 1–102.
[Hall] M. HALL, "The Theory of Groups," Macmillan, New York, 1959.
[Hup] B. HUPPERT, "Endliche Gruppen I," Springer-Verlag, Berlin, 1968.
[Jac] N. JACOBSON, "Structure and Representations of Jordan Algebras," Amer. Math. Soc., Providence, RI, 1968.
[Os] M. OSBORN, Ph.D. thesis, Yale University.
[Rac1] M. RACINE, On maximal subalgebras, *J. Algebra* **30** (1974), 155–180.
[Rac2] M. RACINE, Maximal subalgebras of exceptional Jordan algebras, *J. Algebra* **46** (1977), 12–21.
[Sah] CHIH-HAN SAH, Cohomology of split group extensions, *J. Algebra* **29** (1974), 255–302.
[St] R. STEINBERG, Generators, relations and coverings of algebraic groups, *J. Algebra* **71** (1981), 527–543.